MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 1, 2018/2019

TPB3141 – PASSWORD AUTHENTICATION AND BIOMETRICS

(All sections / Groups)

20 OCTOBER 2018
9.00 a.m – 11.00 a.m
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This question paper consists of 7 pages, excluding the cover page, with 5 questions only.

2. Attempt **ALL** questions. All questions carry equal marks and the distribution of the marks for each question is given.

3. Please print all your answers in the Answer Booklet provided.

Question 1:

Please attempt **ALL** multiple choice questions. [12 marks]

1. _____ occurs when a user (or any subject) claims or professes an identity. This can be accomplished with a username, a process ID, a smart card, or anything else that can uniquely identify a subject.
    a. Authorization
    b. Authentication
    c. Identification
    d. Validation

2. _____ biometric verification methods include keystroke dynamics, gait analysis, voice ID, mouse use characteristics, signature analysis and cognitive biometrics.
    a. Biological
    b. Physiological
    c. Behavioral
    d. Geolocation

3. Fingerprint _____ refers to the automated method of identifying and verifying the identity of an individual based on the comparison of two fingerprints. It is one of the most well-known biometrics, and it is by far the most used biometric solution for authentication on computerized systems.
    a. identification
    b. verification
    c. recognition
    d. authorization

4. _____ impressions are the ten individually-taken fingerprint images rolled from nail to nail. The plain impressions are used to verify the sequence and accuracy of the rolled impressions.
    a. Live
    b. Identification flat/ slap
    c. Rolled
    d. Laser-penetrated

Continued .....

5. _____ speaker recognition characterizes a speaker recognition task, such as verification or identification, in which the set of words (or lexicon) used during the testing phase is a subset of the ones present during the enrollment phase.
   a. Text-filtered
   b. Text-independent
   c. Text-dependent
   d. Text-prompted

6. If the user is aware that a biometric identifier is being measured, the user is _____. If unaware, the use is _____. Almost all conceivable access control and non-forensic applications are _____.
   a. cooperative; non-cooperative; covert
   b. habituated; non-habituated; overt
   c. overt; covert; overt
   d. attended; non-attended; covert

7. It is unknown whether the subject presented to the biometric system for recognition has enrolled in the system or not. Therefore, the system needs to decide whether to reject or recognize him as one of the enrolled subject.
   a. Open-set verification
   b. Closed-set verification
   c. Closed-set identification
   d. Open-set identification

8. _____ is a plastic card with a built-in microprocessor, used typically to perform financial transactions and automatically associated with authentication.
   a. Laser card
   b. Dumb card
   c. Magnetic stripe card
   d. Smart card

Continued .....

9. A _____ is a process that guarantees that the contents of a message have not been altered in transit. When you, the server, digitally sign a document, you add a one-way hash (encryption) of the message content using your public and private key pair.
    a. salting
    b. hashing certificate
    c. digital certificate
    d. digital signature

10. Cryptography is a science of data encryption providing its _____ and _____. After cryptographic transformations (the basis of encryption algorithms) are applied, only the users that possess a relevant key can have access to the initial text.
    a. confidentiality; availability
    b. integrity; availability
    c. non-repudiation; integrity
    d. confidentiality; integrity

11. _____ is an international standard-setting body composed of representatives from various national standards organizations. Founded on 23 February 1947, the organization promotes worldwide proprietary, industrial and commercial standards.
    a. American National Standards Institute (ANSI)
    b. National Institute of Standards and Technology (NIST)
    c. Interagency Advisory Board (IAB)
    d. International Organization for Standardization (ISO)

12. _____ specified criteria for rating the security of different security systems, specifically for use in the government procurement process.
    a. Transport Layer Security (TLS)
    b. Secure Sockets Layer (SSL)
    c. Secure Electronic Transaction (SET)
    d. The Orange Book

Continued .....

Question 2:

a) Fill in the blanks with the most appropriate basic criteria for biometric security system:

i. _____: this information must be as dissimilar as possible for two different individuals.
ii. _____: it should be present during the whole life of an individual.
iii. _____: it can be measured in an easy manner.
iv. _____: it concerns the possibility of a real use by users.
v. _____: all individuals must be characterized by this information.

[5 marks]

b) As part of a nationwide banking industry initiative, the PIN (Personal Identification Number) has been completely replacing your signature for payment transaction authorization since 2017 in Malaysia. A PIN should be entered, instead of signing, when making a card payment at a point-of-sale terminal in Malaysia. The reliability of PIN is relatively poorer than biometrics (signature in this case), but why it is chosen instead? Discuss your opinions toward this new implementation in Malaysia.

[5 marks]

c) Single Sign-On (SSO) is similar to Password Synchronization. Do you agree on this statement? Explain your answer.

[2 marks]

Continued .....

Question 3:

a) In information security, the concepts of identification, authentication and authorization are intertwined, but have specific differences. Define **THREE [3]** of them, and explain each of their application with an example.

[6 marks]

b) In Windows 10, the "*passwords must meet complexity requirements*" policy setting determines whether passwords must meet a series of guidelines that are considered important for a strong password and ensuring the password strength.

With your best knowledge, explain what is password strength?

[2 marks]

c) Biometrics systems are designed to identify or verify the identity of people by using their intrinsic physical or behavioral characteristics. But the privacy risks that accompany biometrics databases are extreme. Identify and briefly describe the **TWO [2]** types of privacy concerns associated with biometrics.

[4 marks]

Continued .....

Question 4:

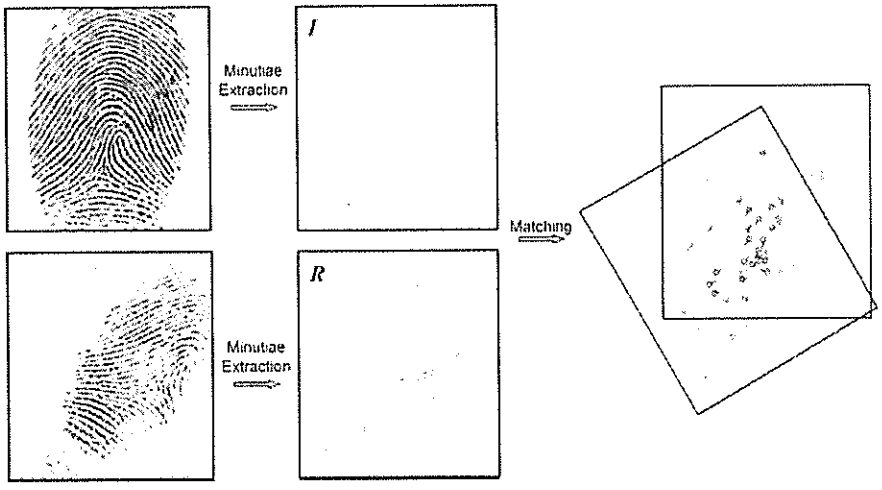
a) In MMU, students have to login to lab computers by using their own Camsys accounts. With the intruder lockout mechanism in place, students are allowed for 3 trials. If students are entering the wrong passwords for 4 times in a row, their accounts will be locked. This can be used to carry out a denial of service (DOS), where the attacker can purposely entering a wrong password for a student, and causing his or her account to be locked. Thus, suggest **THREE [3]** best practices to limit the enforcement of intruder lockout.

[3 marks]

b) Tracking assets is the most obvious application for IoT in the supply chain. RFID tags and chips, along with global SIM cards, are helping supply chain managers, vendors and support entities keep a closer eye on their shipments. Not merely with batch or skid numbers, either, but now with extremely detailed data down to individual products. One implication is the ability of managers to make up-to-the-minute decisions about equipment movement and shipment rerouting based on movement and environmental data gathered out in the field. How does the application of RFID made this possible? Use a picture illustration to explain your answer.

[6 marks]

c) Refer to the figure below, if the matching score of observed minutia patterns (***I*** and ***R***) is 95%, can we deem that the verification rate is also 95%? Can you calculate the value of Equal Error Rate (EER) based on this figure? Explain your answer.



[3 marks]

Continued .....

Question 5:

a) Spoken passwords are all well and good until someone makes a recording of you speaking, or a talented impressionist impersonates you. One extra safeguard to make sure that the pass code speaker is really you?

Propose **ONE [1]** biometric solution to verify the person who speaks the password is the genuine user. Justify your answer.

[4 marks]

b) If you intend to passively verify the students who attending online exam are the legitimate registered students and not someone else, what will be the best behavioral biometric authentication solution? Justify your answer.

[4 marks]

c) When new photos are uploaded, Facebook compares faces present in the image to templates of relevant users and suggests a tag if there's a match. Due to this feature, Facebook is currently being sued for allegedly violating Illinois' Biometric Information Privacy Act (BIPA). The plaintiffs claim that Facebook's widespread collection of face data violates BIPA. Facebook fired back, saying that while they do scan for face templates, this collection doesn't actually harm anyone.

Discuss your opinions from the perspective of privacy continuum.

[4 marks]

End of Page